La conservation de la signature électronique : perspectives archivistiques

Rapport de Jean-François Blanchette remis à la DAF en 2004

Présentation Groupe PIN – 22 mars 2005

Contexte

- Rapport rédigé à la demande de la direction des Archives de France par Jean-François Blanchette chercheur aujourd ’hui maître de conférence à l ’université d ’UCLA enseignant les systèmes d ’information à de futurs bibliothécaires, archivistes et documentalistes
- A fait une thèse sur la signature électronique et travaillé avec les Archives sur le projet de décret d ’application sur les actes authentiques (décret d ’application de la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l ’information et relative à la signature électronique)

Contexte

- Désormais un document électronique a même valeur probante qu ’un document papier, à condition que son auteur puisse être précisément identifié et qu ’il soit établi et conservé dans des conditions de nature à en garantir l ’intégrité (article 1316-1 du Code Civil)
- Dès lors, introduction de la signature électronique et plus précisément, dans le cadre de la directive européenne du 13 décembre 1999, la signature fondée sur la cryptographie a-symétrique qui bénéficie, sous certaines conditions, d ’une présomption de fiabilité.

Contexte

- Or, les conditions de conservation de cette sorte de signature, dans le temps, ne sont nulle part spécifiées
- Ou plutôt on se retrouve face à une contradiction : cette technique permet de déceler toute modification d ’un document (respect de l ’intégrité du document). Or, à plus ou moins longue échéance, des migrations de format seront nécessaires pour préserver la lisibilité du document, migrations qui feront échouer la procédure de vérification de la signature : intégrité contre lisibilité.
- En outre, ces technologies impliquent des infrastructures très lourdes et d ’autant plus lourdes que le temps passe et dont on ignore si les services publics d ’archives pourront les prendre en charge.

Les technologies de signature numérique

- Il se découpe en 4 grandes parties.
- Première partie : description des technologies de signature numérique
  - contexte : science des cryptologues
  - découverte su système cryptographique à clé publique (double clé)
  - application de cette technologie pour la signature d ’un document (permet de déterminer son origine et de s ’assurer qu ’il n ’a pas été modifié)

Les technologies de signature numérique

- Principe de la certication
  - permet par la biais d ’un certificat, de relier une clé publique à son propriétaire
  - ce que recouvre en terme de fonctionnalités une infrastructure à clé publique (PKI en anglais)
  - C ’est l ’explosion des technologies de l ’internet qui fera le succès de ces techniques

Le cadre juridique de la signature électronique

- C ’est la deuxième partie du rapport
- Directive européenne du 13 décembre 1999
  - pose déjà les grands principes
  - annonce une signature dite avancée qui se voit attribuer une force probante supérieure (par opposition à une signature simple) : en fait celle reposant sur les technologies cryptographiques

Le cadre juridique de la signature électronique

- Emergence et adoption de la loi du 13 mars 2000
- introduction d ’une définition de l ’écrit (indépendance entre un écrit et un support) et de la signature (identification de l ’auteur et manifestation de sa volonté)
- introduction d ’une présomption de fiabilité « lorsque la signature est créée, l ’identité du signataire assurée et l ’intégrité de l ’acte garanti ».
- Introduction en outre des actes authentiques dans la loi (le projet ne prévoyait que les actes sous seing privé) soit notamment les minutes notariales, les minutes de jugements, les actes d ’état civil…, avec une accentuation de l ’importance de la signature (confère l ’authenticité) ce

Stratégies techniques pour la conservation de la signature

- Constitue la troisième partie du rapport
  - Distingue bien ce qui relève de la vérification immédiate par le destinataire, de celle pouvant intervenir des années plus tard, par exemple par un juge dans le cadre de contentieux
  - On se heurte alors au problème de l ’obsolescence conjuguée des matériels, logiciels et formats.
  - Or, on doit pouvoir d ’une part disposer d ’équipements permettant d ’accéder aux informations binaires du document sur son support physique, de les décoder et de les rendre manifestes sur papier, sur écran ; et, d ’autre part, pouvoir disposer d ’équipements permettant d ’accéder à la signature électronique sur son support physique, de la décoder et d ’exécuter l ’algorithme de vérification qui permet de déterminer la validité de la signature.

Stratégies techniques pour la conservation de la signature

- Les solutions techniques proposées sont de trois ordres :
  - la re-signature, dès lors que les tailles des clés ne semblent plus suffisantes pour assurer la sécurité. Toutes les étapes du processus de vérification sont explicités dans le rapport permettant de mieux comprendre tous les éléments dont il convient de disposer si on veut « re-jouer » la signature sur le long terme (notamment problématique des certificats qui ne sont valables que pour une période donnée)

Stratégies techniques pour la conservation de la signature

- Autre possibilité : l ’émulation mais elle reste largement expérimentale
- Enfin la canonicalisation qui a pour principe de migrer le document vers un format plus pérenne (format XML canonique) avant de le signer, afin d ’éviter de futures migrations.

Stratégies techniques pour la conservation de la signature

- Aucune de ces solutions ne permet de résoudre le problème :
  - la première ne pose pas le problème de la conservation simultanée du document et de sa signature
  - la seconde reste expérimentale
  - la troisième ne permet que de repousser le problème dans le temps

Réponses apportées par les grandes institutions d ’archives étrangères

- Archives nationales américaines ont publié des recommandations dès 2000 :
  - si une administration veut conserver outre le contenu, le contexte et la structure d ’un document, la préservation de celui-ci implique de respecter l ’intégrité physique et logique du document et par conséquent, de conserver les équipements matériels et logiciels ayant servi à la création de la signature afin que le document puisse être validé à postériori

Réponses apportées par les institutions d ’archives étrangères

- USA
  - si l ’administration ne juge pas indispensable de conserver également la structure du document (ce que les archives recommandent pour les documents à longue durée d ’utilité administrative), dans ce cas, les Archives prescrivent la conservation des informations contextuelles permettant de documenter l ’existence et la validité de la signature ainsi que les mécanismes en place au moment de la signature.

Réponses apportées par les institutions d ’archives étrangères

- USA : dans tous les cas, doivent être enregistrés en clair dans le document le nom du signataire en toutes lettres, sa qualité ainsi que la date de la signature.

Réponses apportées par les institutions d ’archives étrangères

- Australie (recommandations en 2004)
  - recommande si le risque juridique est nul ou faible, de se contenter de conserver les métadonnées sur la signature : identifiant du certificat et de l ’organisation qui l ’a émis, informations relatives à la signature proprement dites comme l ’algorithme, la date et l ’heure où signature apposée, vérifiée

Réponses apportées par les institutions d ’archives étrangères

- Australie
  - à l ’inverse si le risque est élevé, c ’est aux administrations d ’implanter un plan de gestion de clés : conservation de tous les certificats successifs, jetons d ’horodatage, listes de révocations, audits du système.
  - Lors de leur transfert aux AN, celles-ci déclarent ne pas pouvoir assurer la conservation de l ’ensemble de ces éléments mais s ’assurent par contre de la conservation de toutes les

Réponses apportées par les institutions d ’archives étrangères

- Canada : dès le transfert aux Archives, la signature cessera d ’être utile en tant que moyen de preuve
- l ’authenticité des documents reposera plutôt sur leur histoire, leur positionnement au sein de leur système d ’information dans le cadre des activités de l ’organisation, sur les éléments de contexte et de traçabilité accompagnant le document tout au long de

Conclusions

- Il convient par conséquent :
  - de recommander aux administrations de bien déterminer quelles sont les catégories de documents méritant, au regard des contentieux, une conservation de leur contenu, contexte et structure au-delà d ’une durée de 1 à 3 ans
  - s ’ils en existent, les enjoindre de mettre en place le temps qu ’ils jugeront nécessaire, un plan de gestion des clés

Conclusions

- Dans tous les cas, demander à ce que soit enregistrés et figurent dans le document l ’identification en clair du signataire, ainsi que la date et l ’heure de la signature
- Dans tous les cas, conserver les informations contextuelles concernant les signatures (voir recommandations australiennes)
- ne pas assurer, à partir du transfert aux Archives, la prise en charge de ces mécanismes (on ne pourra plus re-jouer les signatures). Position raisonnable étant donné le peu de chances d ’avoir à rejouer une signature des années après son apposition (le risque ne vaut pas les coûts) mais plutôt faire reposer la preuve sur un faisceau d ’indices, fondées sur la pratique archivistique.

Liens

- National Archives and Records Administration (2000), « Records Management Guidance for Agncies Implementing Signature Technologies », Waschington, DC, October 2000
- National Archives of Australia (20004), « Recordkeeping and Online Security Process : Guidelines for Managing Commonwealth Records Created or Reveided Usins Authentification or Encryption », http://www.naa.gov.au/recordkeeping/er/security.html
- Bibliothèque et Archives Canada (2001), « Lignes directrices concernant les documents chiffrés et signés numériquement selon une Infrastructure à clé publique », http://www.collectionscanada.ca/06/0618_f.html
- Rapport de JF Blanchette, sur le site de la direction des archives de France : http://www.archivesdefrance.culture.gouv.fr/fr/textenorme/index.html